Solution Brief

Thales TCT Commercial Solutions for Classified (CSfC) Capabilities

Cyber Security Solutions Support All Capabilities Packages

thalestct.com

THALES
Building a future we can all trust

THALES

What is CSfC?

Commercial Solutions for Classified (CSfC) is a program that enables commercial products to be used in layered solutions to protect classified information. This speeds up the deployment timeline so that a solution can be fielded in months, versus years. The program was designed to allow simultaneous use of multiple unclassified commercial-off-the-shelf (COTS) products instead of classified, Type 1 U.S. Government accredited products to secure classified data within government deployments.

CSfC promotes the protection of critical data with layered encryption technologies. A layered encryption approach is most effective when each layer can stand independently relative to their design, implementation, and operational deployment. There are currently four approved CSfC Capability Packages (CP), each of which outlines overall customer solution architecture requirements as well as specific device configurations.

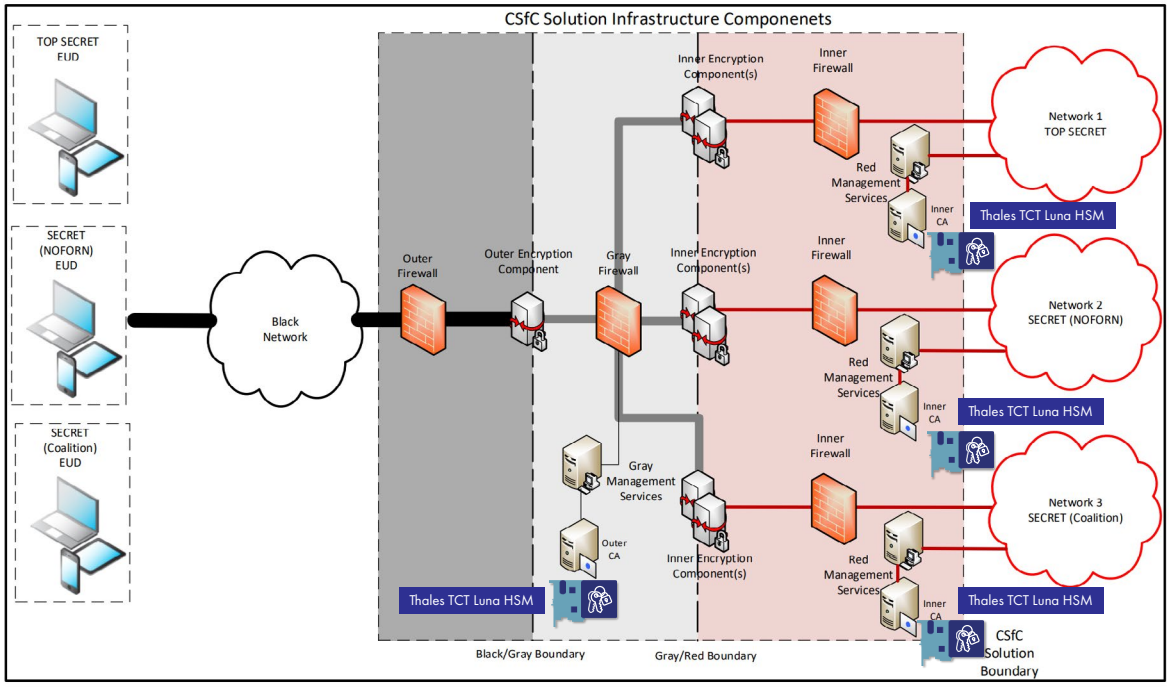
As a longtime provider of cyber security solutions to the U.S. Federal Government, Thales Trusted Cyber Technologies (TCT) is strategic contributor to CSfC solutions. Thales TCT has a rich history of supplying Hardware Security Modules (HSMs) to secure the cryptographic keys used by CSfC Certificate Authorities (CA). Thales TCT's CipherTrust Data Security Platform offers multiple security technologies that align with the CSfC requirements. Thales High Speed Encryptor family of products support a nested configuration that provides layered network encryption as architected in CSfC. And, Thales Multi-factor Authentication (MFA) solutions address CSfC Mobile Access solution requirements.

Hardware Security Modules Secure PKI

Following the CSfC security principles of using multiple independent security layers, the CSfC Key Management Requirements Annex describes the need to implement at least two separate Certificate Authorities (CA) running on separate machines and networks for issuing the PKI certificates within the solution.

For CSfC solutions that support multiple classified enclaves, each enclave must have a separate Inner CA to ensure cryptographic isolation of the enclaves. Use of an HSM to secure the CA private keys is not only identified as best-practice, it is specifically required per the CSfC Key Management Requirements Annex. Due to the separation requirements, each CA uses a dedicated HSM to hold its private key. This is illustrated in the following diagram from the CSfC Key Management Requirements Annex, modified to show the location of an HSM with each CA.

Thales TCT Luna HSMs integrate with industry-leading technology vendors to provide seamless solutions that meet the stringent security requirements established by the U.S. Government. We provide fully vetted, step-by-step integration guides for our broad partner ecosystem of out-of-the-box integrations. As part of the Thales TCT Technology Partner Program, Thales TCT provides extensive and ongoing technical integration support for the products listed on the CSfC approved Certificate Authority Components List.



KM-12 (Key Management Requirements Annex): Private keys associated with on-line (i.e., CA is network-accessible), Outer and Inner CAs must be protected using HSMs validated to Federal Information Processing Standards (FIPS) 140-2/3 Level 2 or greater.

Ref. National Security Agency CSfC Key Management Requirements Annex v2.1, Figure 5

CipherTrust Data Security Platform

The CipherTrust Data Security Platform integrates data discovery, classification, data protection, and unprecedented granular access controls, all with centralized key management. This solution removes data security complexity, accelerates time to compliance, and secures cloud migration, which results in less resources dedicated to data security operations, ubiquitous compliance controls, and significantly reduced risk across your organization. The CipherTrust Data Security Platform simplifies data security administration with a 'single pane of glass' centralized management console that equips organizations with powerful tools to discover and classify sensitive data, combat external threats, guard against insider abuse, and establish persistent controls, even when data is stored in the cloud or in any external provider's infrastructure. The following products within the CipherTrust Data Security Platform are ideally suited for use in CSfC solutions.

CipherTrust Key Generation Solution for Quantum Resistance

The looming cybersecurity threats from cryptographically relevant quantum computers have driven agencies to take immediate action to protect long-life data. In the case of CSfC, quantum resistant cryptographic protection of classified information is accomplished using properly configured, maintained, and monitored CSfC solutions as defined in the CSfC Symmetric Key Management Requirements Annex.

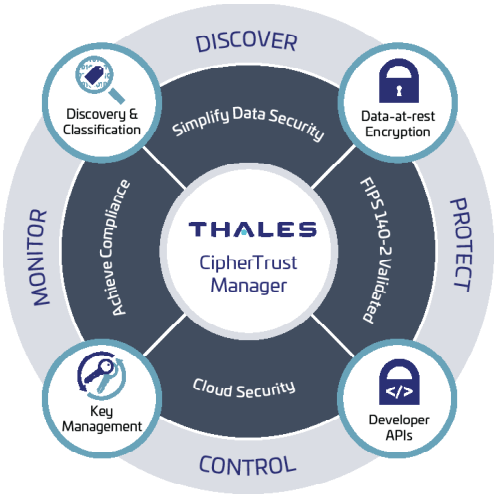
A fundamental component of Symmetric Key Management is use of an NSA approved Key Generation Solution (KGS) for generation and management of Pre-Shared Keys (PSKs) used by the CSfC security devices. Specifically, the KGS is responsible for full lifecycle management of the symmetric PSKs distributed to the security devices running the IPsec and MACsec protocols. With FIPS approved random number and key generation, robust key management capability, management and cryptographic APIs, and detailed auditing and reporting, the CipherTrust KGS meets all of the KGS requirements in the Symmetric Key Management Requirements Annex. CipherTrust KGS has a proven ability to generate and deliver PSKs to CSfC security devices and can be NSA approved as a component of a CSfC registered solution.

CipherTrust Transparent Encryption

CipherTrust Transparent Encryption delivers data at rest encryption, privileged user access controls, and detailed data access audit logging. Agents protect data in files, volumes, and databases on Windows, AIX, and Linux operating systems across physical and virtual servers in cloud and big data environments. The Live Data Transformation extension is available for CipherTrust Transparent Encryption, providing zero-downtime encryption and data rekeying. CipherTrust Transparent Encryption provides a software file encryption capability that aligns with the CSfC Data at Rest Capabilities Package.

CipherTrust Key Management

CipherTrust Key Management delivers a robust, standards-based solution for managing encryption keys across the enterprise. It simplifies administrative challenges around encryption key management to ensure that keys are secure and always provisioned to authorized encryption services.



CipherTrust Key Management solutions support a variety of use cases including cloud key management, database key management, and KMIP key management. CipherTrust Key Management integrates with industry-leading data at rest encryption solutions that are on the CSfC Components List.

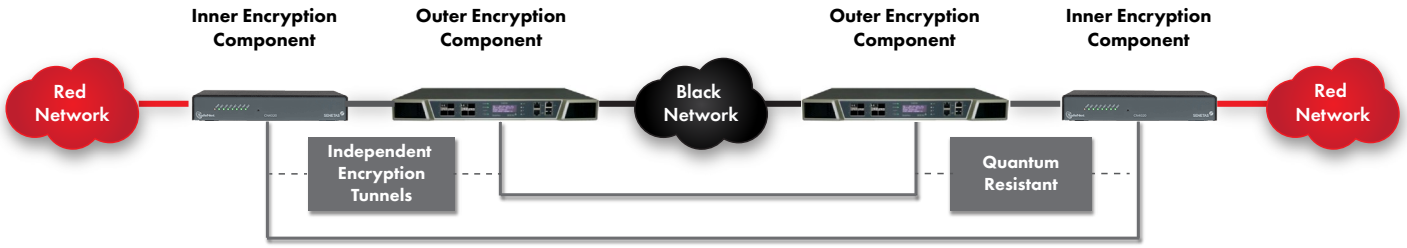
CipherTrust Manager

CipherTrust Manager is the central management point for the platform. It is an industry-leading enterprise key management solution that enables organizations to centrally manage encryption keys, provide granular access controls, and configure security policies. CipherTrust Manager provides role-based access control to keys and policies; manages key lifecycle tasks, including: generation, rotation, destruction, import and export; supports robust auditing and reporting; and offers development and management-friendly REST APIs. CipherTrust Manager is available in physical and virtual form factors that are FIPS 140 compliant up to Level 3 and can be rooted by Thales TCT's T-Series HSMs or removable token HSMs.

Nested High Speed Network Encryption

Thales High Speed Encryptors (HSE) offer a multi-site connectivity solution that not only provides multiple layers of encryption as required by CSfC, but does so while providing significant performance benefits over typical IPsec / MACsec solutions. Thales HSEs deliver deterministic wire speed encryption with microsecond latency and supports up to 100 Gbps throughput per device. Furthermore, Thales HSEs are quantum safe and FIPS 140 certified to operate in a hybrid classic/quantum mode of operation.

Not all encryption solutions are created equal. There are different protocols and modes of operation that affect the performance, efficiency, and security of network encryption. Thales HSEs use a tunnel-free mode that encrypts only the data portion of the packet with minimal overhead and changes to the packet structure. This approach delivers higher performance and lower latency than IPsec. Cut-through packet processing means that the encryptor only needs to receive a few bytes of the header to look up policy and start encrypting data without waiting for the rest of the packet to arrive. Thales HSEs are also vendor-agnostic and can work with any network device or protocol without requiring any changes to the existing infrastructure.



Nested High Speed Network Encryption

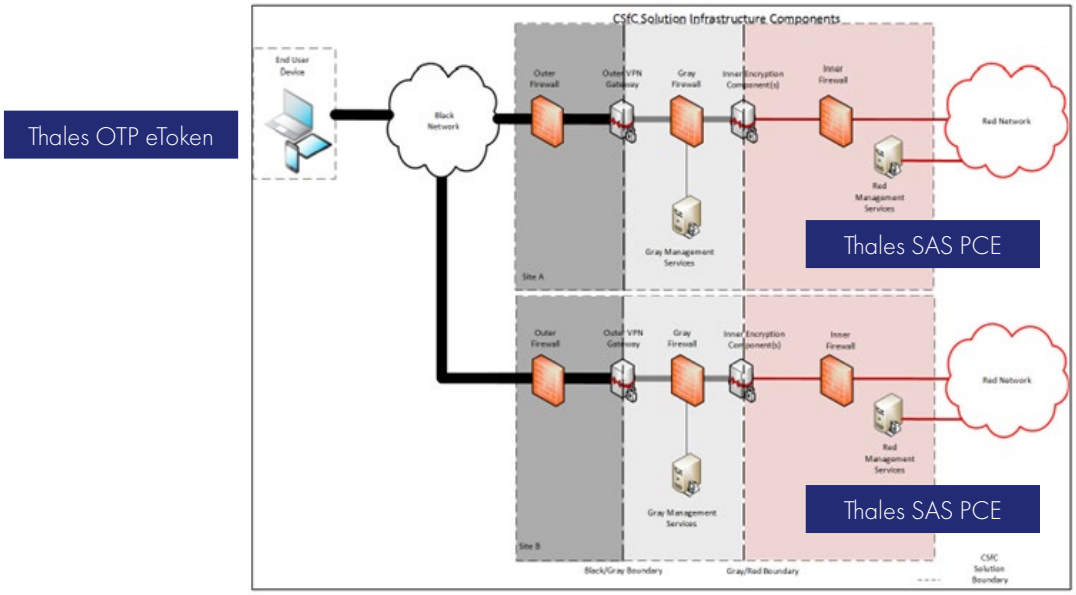
Multi-Factor Authentication

The CSfC Mobile Access (MA) solution provides mutual device authentication between Outer VPN components and between Inner Encryption components via public key certificates. There are two scenarios within the MA CP for multi-factor (aka two factor) authentication: "User to EUD" and "EUD to Infrastructure."

Both the User to EUD and the EUD to Infrastructure MFA requirements summarized in sections 4.4.2.1 and 4.4.2.2 of the CP MA describe use of a physically separate token to serve as the "something you have" factor of the MFA solution. Listed as objective requirements in v2.5.1 of the MA CP, most approved CSfC solutions have yet to integrate token based MFA in fielded solutions.

However, changes in the MA CP to elevate the MFA requirement to the threshold level will necessitate integration of One Time Password (OTP) token based MFA.

Thales OTP authenticator devices teamed with the Thales SafeNet Authentication Service (SAS) PCE Identity Provider (IDP) application provide a mature and well tested solution to directly address these CSfC requirements. The Thales MFA solution meets all 12 requirements detailed in Table 28: EUD to Infrastructure Multi Factor Authentication Requirements. Similarly, the Thales MFA solution meets all of the requirements allocated to OTP MFA tokens in Table 29: User to EUD MFA Requirements. The following diagram illustrates how Thales OTP tokens integrate at the EUD (as an EUD or VPN authenticator) and the corresponding SAS PCE server resides in the management network.



Ref. Overview of Mobile Access Solution, Figure 1

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., protects the most vital data from the core to the cloud to the field. We serve as a trusted, U.S. based source for cyber security solutions for the U.S. Federal Government. Our solutions enable agencies to deploy a holistic data protection ecosystem where data and cryptographic keys are secured and managed, and access and distribution are controlled. For more information, visit www.thalestct.com